REMARKS

I. INTRODUCTION

In response to the Office Action dated August 15, 2006, claims 1, 15, 30, and 45 have been amended and claims 14, 29, 44, and 59 have been cancelled. Claims 1-10, 12-13, 15, 17-25, 27-28, 30-40, 42-43, 45, 47-55, and 57-58 remain in the application. Entry of these amendments, and reconsideration of the application, as amended, is requested.

II. CLAIM AMENDMENTS

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for patentability or to distinguish the claims over the prior art.

III. NON-ART REJECTIONS

In paragraph (4) of the Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 58 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. In paragraph (5) of the Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 58 were rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections.

Applicants respectfully traverse the above rejections.

With respect to claims 12, 13, 27, 28, 42, 43, 57, and 58, the claims were rejected stating that while the specification suggests the use of multiplexors with the hardware state machine, nowhere is it described in the manner in which the multiplexors are actually used or configured. The rejections further state that it is unclear how the multiplexors relate to the remainder of the invention.

In the prior response, Applicants referred the Examiner to paragraphs [0070] 0074]:

> **[0070]** The hardware state machine 718 may contain the same logic as used in the prior art and may not be modified. In addition to the state machine 718, the implementation consists of a permutation that employs a series of configurable multiplexors at the beginning 716 and end 720 of the fixed hardware state machine 718. Custom logic (i.e., the logic within hardware configuration control and IO module 714) interconnects the multiplexors (within permutations 716 and 720) to the system bus 612 of CAM 512. Accordingly, the hardware configuration control and IO module 714 that connects to the system bus 612 controls access to the permutation 716 and 720 and state machine 718 logic.

[0071] The custom logic within the control and IO module 714 implements a key exchange protocol by accepting (or rejecting) a series of pre-authorized keys (e.g., sequentially wrapped keys with $n=10^6$ times or other large value) or other secure protocol. The key defines a configuration for the permutations 716 and 720. Valid keys are only known to the headend (e.g., uplink center 104) by using any public key algorithm such as Rabin or RSA (Rivest-Shamir-Adelman). Based on a public key algorithm, the keys cannot be recreated or generated by unknown parties. The keys are delivered to the smart card either over the broadcast stream, Internet, or other appropriate distribution channel. The keys can be delivered to the smart card (i.e., CAM 512) population asynchronously (e.g., over a period of several hours, days, or months). The keys may be delivered using uniquely encrypted, group encrypted packets. These packets are unintelligible to members (i.e., CAMs 512) for which they were not encrypted. In other words, the packets are only intelligible to those members/control and IO modules 714 having the appropriate private key.

[0072] The hardware configuration control and IO module 714 verifies/authenticates the key. Such a verification/authentication may ensure that the key is from a known source (e.g., a known uplink center 104, program source 200A-200C,etc.), that the key is not a duplicate of an already received key, or that the key fails to comply with an additional security measure. As part of the authentication process, the control and IO module 714 decrypts the keys. The decrypted key is then verified/authenticated by the custom logic within module 714. If the key is valid, the key is retained by the control and IO module 714 (e.g., by storing the keys in protected registers with no physical or logical output mechanism outside the custom logic within the module 714). If the key is invalid, the key is rejected and may not be stored by the control and IO module 714.

[0073] As described above, the key defines a configuration for the permutations 716 and 720. Accordingly, when appropriate, the key is used to dynamically (i.e., on-the-fly) reconfigure the permutations 716 and 720. The timing of the reconfiguration may occur immediately upon receipt of the key. Alternatively, the key may be stored by control and IO module 714 and only used to reconfigure the permutations 716 and 720 (e.g., switch the configuration to that represented by the stored key) upon receipt of an over the air command. In such a circumstance, the control and IO module 714 may store a currently active key (that defines a permutation 716 and 720 currently being used) and a future key. Accordingly, the keys may be delivered asynchronously over a very long period of time to multiple CAMs 512 where they are validated and stored asynchronously. Thereafter (e.g., once a period of time has passed to ensure that appropriate/enough CAMs 512 have the new key), an over the air command to activate a reconfiguration operation for a key may be delivered synchronously to all CAMs 512. Thus, the actual reconfiguration operation may occur simultaneously within all CAMs 512, while the key delivery and validation mechanism is asynchronous over a period of time.

[0074] To recongifure the permutations, 716 and 720, the control and IO module 714 communicates bi-directly 722 with the pre-permutations 716 and post-permutations 720 to dynamically configure the series of multiplexors in each respective permutation 716 and 720. Once configured, the pre-permutations 716 place the digital services information received across communication link 724 from control and IO module 714 into the appropriate form for use by the hardware state machine 718. Hardware state machine 718 may modify the digital services

> information based on custom logic within the state machine 718. Thereafter, the post-permutations 720 may modify the outgoing digital services information to limit use and viewing of the information from unauthorized attackers.

As can be seen, such paragraphs clearly provide that the key is used to configure the series of multiplexors within each permutation. The claims do not recite nor specify that the same number of inputs or outputs are used. Instead, the claims provide for using a series of configurable multiplexors based on the key. Since the multiplexors are configurable, the key may be used to dynamically configure the various components of the invention. Such a use clearly establishes a how the multiplexors relate to the invention.

In addition, Applicants previously provided a standard dictionary definition for a multiplexor that described a rearrangement of elements of a set. Such a definition was merely ignored in the final Office Action. Applicants now provide yet another definition from wikipedia – "http:en.wikipedia.org/wiki/Demultiplexor". The definition provides "It is usual to combine a multiplexor and a demultiplexor together into one piece of equipment and simply refer to the whole thing as a 'multiplexor'...". Based on such a definition, it is clearly that a multiplexor (that includes both a multiplexor and demultiplexor) can easily be configured to have inputs and outputs that merely permute the data. Nonetheless, the claims do not require an identical number of inputs and outputs as suggested by the Examiner. Instead, the pre-permutation module merely employs a series of configurable multiplexors. Such a teaching is completely related to the present invention.

With respect to enablement, Applicants submit that the use of configurable multiplexers are known in the art. For example, U.S. Patent No. 5,867,644 by Ranson describes how user configurable multiplexer circuitry can be used (See Abstract). Thus, the recitation in the present invention that describes the use of the key to configure the multiplexors in combination with the known use of configurable multiplexors clearly enables the practice of the invention. In addition, as described below, the invention provides unique features and advantages over that of the prior art.

The Office Action asserts that the specification paragraph 70 simply states that the invention connects multiplexers using custom logic. Applicants respectfully disagree and traverse such an assertion. Paragraph 70 is recited above and provides that a permutation employs a series of configurable multiplexors. Further, contrary to that asserted in the Office Action, paragraph 70 states that the custom logic interconnects the configurable multiplexors to the system bus of the CAM. Again, the custom logic utilizes these configurable multiplexors at the beginning and end of the hardware state machine. Further, the above paragraphs specify that a key is used to define the configuration for the multiplexors. The above paragraphs 70-74 provide and describe explicitly how the multiplexors are used in the invention and in fact provide enabling support under 35 U.S.C. 112.

In view of the above, Applicants respectfully request that the rejections under 35 U.S.C. 112 be withdrawn.

IV. PRIOR ART REJECTIONS

In paragraph (5) of the Office Action, claims 15, 17-19, 21-24, 30-34, 36-39, 45, 47-49 and 51-54 were rejected under 35 U.S.C. §102 as being anticipated by Campinos et al., U.S. Patent 6,035,038 (Campinos). In paragraph (6) of the Office Action, claims 1-10, 12, 15, 17-25, 27, 30-40, 42, 45, 47-55 and 57 were rejected under 35 U.S.C. §103(a) as being obvious in view of the combination of Wasilewski et al., U.S. Patent 6,157,719 (Wasilewski) and Campinos.

In addition, claims 14, 29, 44, and 59 were merely objected to as being dependent upon rejected base claims but would be allowable if rewritten.

Specifically, the independent claims were rejected as follows:

> As per claims 1, 2, 15, 30, 31, 45, Wasilewski discloses an access system for set-top boxes wherein configuration information may be transmitted to the set-top box as a one-time event (i.e, asynchronously). Since the set-top box's function is to determine whether an encrypted instance should be decrypted, it constitutes a security component that controls access to digital services. The received configuration information (the EMM) comprises decryption keys (control words) to be implemented (see column 6. line 24 to column 7, line 24) in a hardware state machine (the DHCT) such as an ASIC (see column 15, lines 32-36 and figures 28 and 3). A control suite (the control center) sends transmissions via satellite, which inherently employs an uplink center for sending transmissions to the satellite. The stream is incorporated at a media server for distribution (see column 15, lines 7-24). The system comprises a smart card (see column 21, line 13).
>
> The components of the DHCTSE, which containslhe hardware state machine, are only accessible to the system bus or I10 via the DHCT interface. In Wasilewski's implementation, components of the DHCTSE communicate with one another via a local bus (see figure 12 and column 21, lines 15-27). Campinos discloses a conditional access system wherein access control (the equivalent of the DHCTSE) is preformed on a user smartcard having no local bus and no direct outside access to the access control circuit (see figure 5 and column 5, line 28 to column 6, line 14) and suggests that this card makes it possible to verify that 'entitlements in the EMM are reserved for the user (see column 3, lines 48-57). Therefore it would have been obvious to one of ordinary skill in the art at the timethe invention was made to implement the invention of Wasilewski using the smartcard of Campinos for the DHCTSE, as this card makes it possible to verify that entitlements in the EMM are reserved for the user.

Applicant traverses the above rejections for various reasons. Nonetheless, in the interest of expediting prosecution, Applicants have amended the independent claims to incorporate the limitations of the objected claims. Accordingly, Applicant submit that the Application is in condition for allowance.

V. CONCLUSION

In view of the above, it is submitted that this application is now in good orde:: for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,
Ronald P. Cocchi et al.
By their attorneys,

Date: October 13, 2006

By: ______________________
Name: Georgann S. Grunebach
Reg. No.: 33,179

The DIRECTV Group, Inc.
CA/LA1/A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245

Telephone No. (310) 964-4615